

F3

**ELECTRONIC EQUIPMENT AND METHOD FOR REWRITING INSIDE PROGRAM  
OF THE SAME EQUIPMENT AND COMPUTER READABLE INFORMATION  
STORAGE MEDIUM RECORDED WITH PROGRAM HAVING FUNCTION FOR  
REWRITING THE SAME PROGRAM**

**Publication number:** JP2001092668  
**Publication date:** 2001-04-06  
**Inventor:** SAKAMOTO KAZUYUKI  
**Applicant:** SONY CORP  
**Classification:**  
**- international:** G06F21/22; G06F9/445; G06F15/00; G06F21/20;  
G06F21/22; G06F9/445; G06F15/00; G06F21/20;  
(IPC1-7): G06F9/445; G06F15/00  
**- European:**  
**Application number:** JP19990265843 19990920  
**Priority number(s):** JP19990265843 19990920

**Report a data error here**

**Abstract of JP2001092668**

**PROBLEM TO BE SOLVED:** To provide electronic equipment for ensuring high security related with the writing of an inside program, a method for rewriting the inside program of the electronic equipment, and a computer readable information recording medium for recording program having a function for rewriting the inside program of the electronic equipment. **SOLUTION:** This electronic equipment 1 capable of the rewriting of an inside program for controlling an operation is provided with a storage means 7 for storing the first identifier of a person who has authority to rewrite the inside program, identifying means 2 and 9 for identifying the second identifier of a person who tries to rewrite the inside program, and a certifying means 9 for collating thesecond identifier with the first identifier for certifying.

---

Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-92668  
(P2001-92668A)

(43) 公開日 平成13年4月6日 (2001.4.6)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 6 F 9/445		G 0 6 F 9/06	5 5 0 G 5 B 0 7 6
9/06	5 5 0	15/00	3 3 0 F 5 B 0 8 5
15/00	3 3 0	9/06	4 2 0 M

審査請求 未請求 請求項の数4 O L (全 8 頁)

(21) 出願番号 特願平11-265843

(22) 出願日 平成11年9月20日 (1999.9.20)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 坂本 和之

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100096806

弁理士 岡▲崎▼ 信太郎 (外1名)

Fターム(参考) 5B076 BB14 FA20 FB20

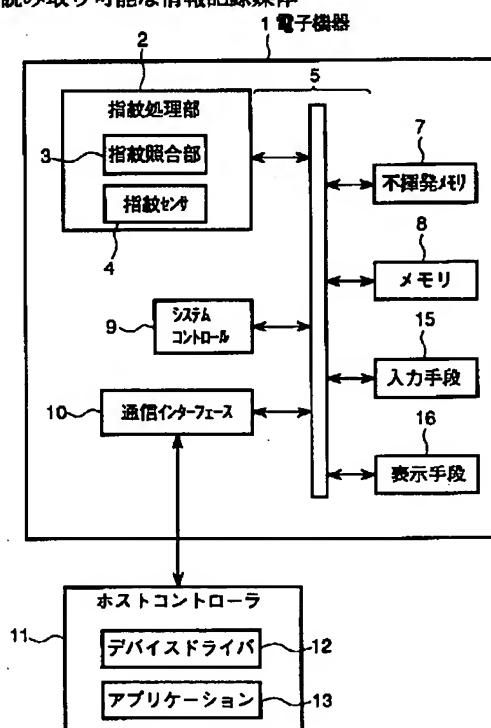
5B085 AED2 AE23 AE26

(54) 【発明の名称】 電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能

(57) 【要約】 を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体

【課題】 内部プログラムの書き換えに関して高いセキュリティを確保することができる電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体を提供すること。

【解決手段】 動作を制御するための内部プログラムを書き換え可能な電子機器1であって、前記内部プログラムの書き換えについて許可されている者の第1識別子を格納する格納手段7と、前記内部プログラムを書き換えようとする者の第2識別子を識別するための識別手段2、9と、前記第2識別子を前記第1識別子と照合し、認証するための認証手段9とを設ける。



【特許請求の範囲】

【請求項1】 動作を制御するための内部プログラムを書き換え可能な電子機器であって、前記内部プログラムの書き換えについて許可されている者の第1識別子を格納する格納手段と、前記内部プログラムを書き換えようとする者の第2識別子を識別するための識別手段と、前記第2識別子を前記第1識別子と照合し、認証するための認証手段とを備えることを特徴とする電子機器。

【請求項2】 前記第1識別子及び前記第2識別子は、それぞれ指紋若しくは暗号キー又はこれらの組み合わせである請求項1に記載の電子機器。

【請求項3】 動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え方法であって、前記内部プログラムの書き換えについて許可されている者の第1識別子を格納手段に格納する格納ステップと、前記内部プログラムを書き換えようとする者の第2識別子を識別手段によって識別するための識別ステップと、前記第2識別子を前記第1識別子と照合し、認証手段によって認証するための認証ステップとを有することを特徴とする電子機器の内部プログラム書き換え方法。

【請求項4】 動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え機能を有する内部プログラムを記録したコンピュータ読み取り可能な情報記録媒体であって、前記内部プログラムの書き換えについて許可されている者の第1識別子を格納手段に格納する格納ステップと、前記内部プログラムを書き換えようとする者の第2識別子を識別手段によって識別するための識別ステップと、前記第2識別子を前記第1識別子と照合し、認証手段によって認証するための認証ステップとを有する電子機器の内部プログラム書き換え機能を有するプログラムを記録したことを特徴とするコンピュータ読み取り可能な情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、書き換え可能な内部プログラムによって動作が制御されている電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体に関するものである。

【0002】

【従来の技術】 近年、産業の発達によって電子機器には、様々な機能が搭載されている。この電子機器は、例えば所定のファームウェア（内部プログラム）によってその機能を発揮するように制御されている。このファームウェアは、例えば電子機器に内蔵するメモリに格納されている。このメモリは、例えばデータの書き換えが可

能であり、電子機器は、このファームウェアを書き換えることによってその機能を変更することができる。従来、このファームウェアは、特定の者によってのみ書き換えられるように、例えばパスワードや電子機器のシリアル番号を入力させるといった簡易な認証手段によって認証させていた。

【0003】

【発明が解決しようとする課題】 ところが、このようなパスワードや電子機器のシリアル番号等の情報が一旦漏洩してしまうと、ファームウェアが第三者によって不正に書き換えられてしまう問題点があった。つまり、第三者が、ファームウェアの動作中（以下、「オンライン」という）にファームウェアを書き換えてしまうと、電子機器は正常な動作を行わない場合があった。

【0004】 そこで本発明は上記課題を解消し、内部プログラムの書き換えに関して高いセキュリティを確保することができる電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体を提供することを目的としている。

【0005】

【課題を解決するための手段】 上記目的は、請求項1の発明にあつては、動作を制御するための内部プログラムを書き換え可能な電子機器であつて、前記内部プログラムの書き換えについて許可されている者の第1識別子を格納する格納手段と、前記内部プログラムを書き換えようとする者の第2識別子を識別するための識別手段と、前記第2識別子を前記第1識別子と照合し、認証するための認証手段とを備えることを特徴とする電子機器により、達成される。

【0006】 上記目的は、請求項3の発明にあつては、動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え方法であつて、前記内部プログラムの書き換えについて許可されている者の第1識別子を格納手段に格納する格納ステップと、前記内部プログラムを書き換えようとする者の第2識別子を識別手段によって識別するための識別ステップと、前記第2識別子を前記第1識別子と照合し、認証手段によって認証するための認証ステップとを有することを特徴とする電子機器の内部プログラム書き換え方法により、達成される。

【0007】 上記目的は、請求項4の発明にあつては、動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え機能を有する内部プログラムを記録したコンピュータ読み取り可能な情報記録媒体であつて、前記内部プログラムの書き換えについて許可されている者の第1識別子を格納手段に格納する格納ステップと、前記内部プログラムを書き換えようとする者の第2識別子を識別手段によって識別するための識別ステップと、前記第2識別子を前記第1識別子と照

合し、認証手段によって認証するための認証ステップとを有する電子機器の内部プログラム書き換え機能を有するプログラムを記録したことを特徴とするコンピュータ読み取り可能な情報記録媒体により、達成される。

【0008】請求項1、3又は4のいずれかの構成によれば、電子機器は、その動作を制御するための内部プログラムが書き換え可能である。この内部プログラムは、電子機器の動作を制御するためのものである。格納手段には、内部プログラムの書き換えについて許可されている者の第1識別子が格納されている。識別手段は、前記内部プログラムを書き換えようとする者の第2識別子を識別する。認証手段は、識別手段によって識別された第2識別子を格納手段の第1識別子と照合し、認証する。従って、電子機器の内部プログラムは、認証を受けた者のみが書き換えることができるようになる。このため、電子機器は、内部プログラムの書き換えに関してセキュリティを向上させることができる。

【0009】請求項2の発明は、請求項1の構成において、前記第1識別子及び前記第2識別子は、それぞれ指紋若しくは暗号キー又はこれらの組み合わせであることを特徴とする。

【0010】

【発明の実施の形態】以下、本発明の好適な実施の形態を添付図面に基づいて詳細に説明する。なお、以下に述べる実施の形態は、本発明の好適な具体例であるから、技術的に好ましい種々の限定が付されているが、本発明の範囲は、以下の説明において特に本発明を限定する旨の記載がない限り、これらの形態に限られるものではない。以下の説明においては、電子機器1が動作中である状態を「オンライン」という。

【0011】図1は、本発明の第1実施形態としての電子機器1及びホストコントローラ11の構成例を示すブロック図である。ホストコントローラ11は、例えば作業者によって操作されるコンピュータのような電子機器であり、所定の信号線を介して電子機器1に接続されている。ホストコントローラ11は、例えばデバイスドライバ12及びアプリケーションプログラム13（アプリケーション）を有する。ホストコントローラ11は、例えば電子機器1の通信インターフェース10との間でデータの通信制御を行う。

【0012】デバイスドライバ12は、例えばホストコントローラ11の基本動作を制御するためのソフトウェアである。デバイスドライバ12は、電子機器1のファームウェア（内部プログラム）を書き換えるための権利（以下「書き換え権」という）を電子機器1に対して要求する。ここで、「ファームウェア」とは、ハードウェアに組み込まれて動作するプログラムをいう。デバイスドライバ12は、この書き換え権を取得すると、アプリケーション13に対してファームウェアの書き換えコマンドの発行を許可する。尚、ホストコントローラ14

は、デバイスドライバ12が書き換え権の取得に関与せず、アプリケーション13が直接書き換え権の要求を行うような構成であってもよい。

【0013】アプリケーション13は、例えば電子機器1のファームウェアを書き換えるためのコマンドを発行するためのプログラム（電子機器の内部プログラム書き換え機能を有するプログラム）である。デバイスドライバ12及びアプリケーション13は、それぞれ例えば図示しないメモリに記憶されている。

【0014】上記電子機器1は、例えば指紋処理部2（識別手段）、システムコントロール9（識別手段、認証手段）、通信インターフェース10、バス線5、不揮発メモリ7（格納手段）、メモリ8、入力手段15及び表示手段16を有する。バス線5は、例えば指紋処理部2、システムコントロール9、通信インターフェース10、不揮発メモリ7、メモリ8、入力手段15及び表示手段16と接続されている。この電子機器1は、指紋照合器（指紋照合器付きドア等を含む）、携帯型電話装置、情報端末、コンピュータ等の電子機器である。

【0015】指紋処理部2は、例えば電子機器1のファームウェアを書き換えようとする作業者の識別子を識別するための処理を行う。この識別子としては、例えば指紋がある。指紋処理部2は、例えば指紋センサ4及び指紋照合部3を有する。指紋センサ4は、図2のようにLED（Light Emitting Diode）21、プリズム20、レンズ22及び撮像素子の一例としてのCCD（Charge Coupled Device）23を有する。CCD23には、指紋照合部3が接続されている。

【0016】LED21は、電子機器1のファームウェアを書き換えようとしている作業者の指Fが接触しているプリズム400に対して発光する。レンズ22は、指Fの指紋の凹凸情報を表す光信号を集光する。CCD23は、この光信号を電気信号に変換する。指紋照合部3は、この光信号を指紋画像とし、この指紋画像を図1の不揮発メモリ7に予め格納されている指紋画像と照合する。

【0017】システムコントロール9は、例えば電子機器1全体を制御するための制御部である。システムコントロール9は、バス線5を介して接続されている指紋処理部2、通信インターフェース10、不揮発メモリ7、メモリ8、入力手段15及び表示手段16を制御している。システムコントロール9は、例えばホストコントローラ14からのファームウェア書き換え権利の要求に対して応答する。

【0018】通信インターフェース10は、例えばホストコントローラ11との間でデータ通信を行うためのインターフェースである。通信インターフェース10としては、例えばRS-232C、USB（Universal Serial Bus）、赤外線通信、LAN

(Local Area Network) が挙げられる。

【0019】不揮発メモリ7は、書き換え可能な不揮発性の情報記憶媒体であり、例えば電子機器1のファームウェアの書き換え権限が付与された者の識別子、例えば指紋情報を格納している。不揮発メモリ7には、例えば指紋照合用の指紋画像データ、任意の一般データ及びファームウェア、好ましくは電子機器1のファームウェアを書き換える機能を有するプログラム(書き換えプログラム)の一部が格納されている。この書き換えプログラムの一部の機能としては、例えばホストコントローラ14からの書き換え権要求に応答する機能である。

【0020】不揮発メモリ7では、プログラム以外のデータはファイルという単位で分類され、1つ1つのファイルは所有者がわかる識別子を有する。そして、不揮発メモリ7には、電子機器1に対してどのような権限を有するかを上述の書き換えプログラムによって設定することができる。尚、不揮発メモリ7は、複数設けられているような構成であっても良い。この場合、各データは、複数の不揮発メモリのうち、いずれに書いてあっても良い。

【0021】メモリ8は、例えばデータの書き換え可能な揮発性メモリであり、システムコントロール9の制御によって上述の書き換えプログラムが読み込まれ、その書き換えプログラムの作業領域として用いられる。尚、メモリ8は、複数設けられていても良い。入力手段15は、例えば文字等を入力するためのキーボードやマウス等のポインティングデバイスである。表示手段16は、例えば液晶ディスプレイやCRT(Cathode Ray Tube)のような表示装置である。

【0022】電子機器1は以上のような構成であり、電子機器1のファームウェアの書き換え方法について図1～図4を参照しながら説明する。図3は、図1の電子機器1のファームウェアの書き換え方法の一例を示すフローチャートである。作業者は、電子機器1のファームウェアを書き換える作業を行う者である。電子機器1は例えばオンラインであってもファームウェアを書き換えることができるので、特定の作業者のみが許可されるべきである。

【0023】作業者は、電子機器1のファームウェアを書き換える際に、指紋センサ4に所定の指を配置させる。電子機器1は、書き換え処理を開始する(ステップST1)。電子機器1は、図1の指紋処理部2を制御して作業者の指紋画像を取り込む(ステップST2)。不揮発メモリ7には、例えば予め書き換え権限が付与された者の指紋画像に関するデータが格納されている(格納ステップ)。作業者は、例えば不揮発メモリ7に格納されたものであって表示手段16に表示されている指紋画像から最も近いものを入力手段15によって指定する(ステップST3)。

【0024】電子機器1は、両者の指紋が一致しているか否かを判断する(ステップST4:識別ステップ)。一致していないと判断されると、作業者は、ファームウェアの書き換え許可に関する権限(以下、単に「書き換え権限」という)が付与されない。一方、一致していると判断されると、作業者は、さらに書き換え権限を持つ指紋か否かが判断される(ステップST5)。

【0025】作業者は、キーボード等の入力手段15によって予め設定されたパスワードを入力する(ステップST6)。電子機器1は、入力されたパスワードを予め設定されたパスワードと照合し、一致しているか否かを判断する(ステップST8)。一致していないと判断されると、作業者は、書き換え権限が付与されない(ステップST17)。一方、一致していると判断されると、電子機器1は、入力されたパスワードが書き換え権限をもつ者のパスワードであるか否かを判断する(ステップST9)。

【0026】電子機器1が書き換え権限を有する者のパスワードでないと判断すると、作業には、書き換え権限が付与されない。一方、電子機器1が書き換え権限を有する者のパスワードであると判断すると、作業には、書き換え権限が付与される(認証ステップ)。ホストコントローラ11は、システムコントロール9の制御によって通信インターフェース10を用いて、電子機器1のファームウェアを書き換える。従って、作業者は、所定の操作を電子機器1に対して行うことによって電子機器1のファームウェアを書き換えることができる。

【0027】本発明の第1実施形態によれば、予め設定された作業者のみが電子機器1のファームウェアを書き換えることができるので、電子機器1のファームウェアの書き換えに関して従来以上にセキュリティを確保することができる。特に、電子機器1は、オンラインでファームウェアを書き換えることができる場合には、任意の者がファームウェアを書き換えることは好ましくないもので、特に効果を発揮する。また、電子機器1は、ファームウェアの書き換えに関する情報が漏洩した場合であっても、ファームウェアの書き換えに際し予め設定した者の指紋等の照合が必要であるので、ファームウェアの書き換えに関してセキュリティを守ることができる。

【0028】また、電子機器1のファームウェアの書き換え方法は、以下のようなフローチャートに従って動作しても良い。図4は、図3のフローチャートの変形例を示すフローチャートである。図4のフローチャートでは、図3のフローチャートにおいて同一の符号を付した箇所は同じ処理であるから、異なる点についてのみ説明する。尚、図4において影のついている処理(例えばステップST3、ステップST6及びステップST7)は、例えばシステムコントロール9が行っているものとする。

【0029】図4のフローチャートでは、作業者が入力

手段15によって入力したパスワードが、例えば不揮発メモリ7に格納されたパスワードと照合されることである。この不揮発メモリ7に格納されたパスワードは、例えば上述の書き換え権限を付与された者毎に格納されている。

【0030】このような変形例では、上述の手法による効果に加えてさらに、指紋画像の選択等の作業者の操作をシステムコントロール9が代行することで、作業者の操作を簡素化することができる。

#### 【0031】第2実施形態

図5は、本発明の第2実施形態としての電子機器1及びホストコントローラ11の構成例を示すブロック図である。図5では、第1実施形態における図1と同一の符号を付した箇所は同じ構成である。図6は、図1の電子機器1のファームウェアの書き換え方法の一例を示すフローチャートであり、図7は、図6のフローチャートの変形例を示すフローチャートである。図6及び図7では、それぞれ第1実施形態における図3及び図4と同一の符号を付した処理は同じ処理であるから、異なる点についてのみ説明する。

【0032】第2実施形態としての電子機器1aでは、第1実施形態としての電子機器1の構成に暗号処理部6が加えられている。暗号処理部6は、例えば公開鍵暗号法や共通鍵暗号法の暗号／復号化処理を行う。また、作業者の操作面においては、第2実施形態としての電子機器1aでは、第1実施形態としての電子機器1において入力していたパスワードの代わりに、後述する暗号キーを入力している。

【0033】電子機器1aにおけるステップST1～ステップST5の処理は、第1実施形態としての電子機器1のステップST1～ステップST5の処理と同様であるので説明を省略する。ステップST5の処理が終了して、電子機器1aは、識別された作業者の指紋を書き換え権限を有する者の指紋でないと判断すると、作業には書き換え権限が付与されない(ステップST17)。一方、電子機器1aは、識別された作業者の指紋を書き換え権限を有する者の指紋であると判断すると、第1乱数を出力する(ステップST10)。作業者は、入力手段15によって自分の暗号キーで第1乱数を暗号化する(ステップST11)。電子機器1aは、暗号化された暗号文を指定された暗号キーで復号化する(ステップST13)。電子機器1aは、先に出力した第1乱数と、複合化された第2乱数とが一致しているか否かを判断する(ステップST14)。

【0034】電子機器1aは、一致していないと判断すると作業者に書き換え権限を付与しない(ステップST17)。一方、電子機器1aは、一致していると判断すると暗号キーを入力した者が書き換え権限があるか否かを判断する(ステップST15)。電子機器1aは、書き換え権限がない者であると判断すると作業者に書き換

え権限を付与しない(ステップST17)。一方、電子機器1aは、書き換え権限がある者であると判断すると作業者に書き換え権限を与え、第1実施形態と同様に電子機器1のファームウェアを書き換える。

【0035】本発明の第2実施形態によれば、異なる手法であっても第1実施形態とほぼ同様の効果を発揮することができる。

【0036】また、第2実施形態としての電子機器1aのファームウェアの書き換え方法は、以下のようなフローチャートによって動作しても良い。図7は、図6のフローチャートの変形例を示すフローチャートである。図7のフローチャートでは、図6のフローチャートにおいて同一の符号を付した箇所は同じ処理であるから、異なる点についてのみ説明する。尚、図7において影のついている処理(例えばステップST3、ステップST11及びステップST12)は、例えばシステムコントロール9が行っている。図7のフローチャートでは、作業者が入力手段15によって入力したパスワードが、例えば不揮発メモリ7に格納されたパスワードと照合されることである。この不揮発メモリ7に格納されたパスワードは、例えば上述の書き換え権限を付与された者毎に格納されている。

【0037】このような変形例では、上述の手法による効果に加えてさらに、指紋画像の選択等の作業者の操作をシステムコントロール9が代行することで、作業者の操作を簡素化することができる。

【0038】ところで本発明は上述した実施形態に限定されるものではない。例えば、電子機器1、1aは、それぞれ上述の書き換え権限を有する者であるか否かを判断し認証するのに、例えば指紋照合、パスワード照合若しくは暗号照合のいずれか又はこれらいずれかの組み合わせであっても良いことはいうまでもない。

【0039】また、上述の認証機能において認証とは、電子機器1、1aにそれぞれ格納されたデータと、それらの外部から入力されたデータとを照合する動作を示しており、上述のような指紋照合等には限られず他の認証手段によって行われても良い。

【0040】また、電子機器1、1aは、例えばコンピュータや電話装置であっても良いし、上述の指紋処理部2の代わりに図8のようなカード型指紋照合部30が設けられていても良い。

【0041】電子機器1、1aは、例えばドアの側等に付けたセキュリティシステムであっても良い。

【0042】上述の電子機器1のファームウェアを書き換える機能を有するプログラムは、例えばフレキシブルディスクやCD(Compact Disc:商標名)等の情報記録媒体に格納されているような形態でも良い。また、この情報記録媒体としては、そのプログラムがネットワーク上に散在するコンピュータ等の電子機器に記録されたものであって、その電子機器からネットワ

ークを經由してユーザのコンピュータ等の電子機器にダウンロードされる形態のものを含んでも構わない。

【0043】

【発明の効果】以上説明したように、本発明によれば、内部プログラムの書き換えに関して高いセキュリティを確保することができる電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体を提供することができる。

【図面の簡単な説明】

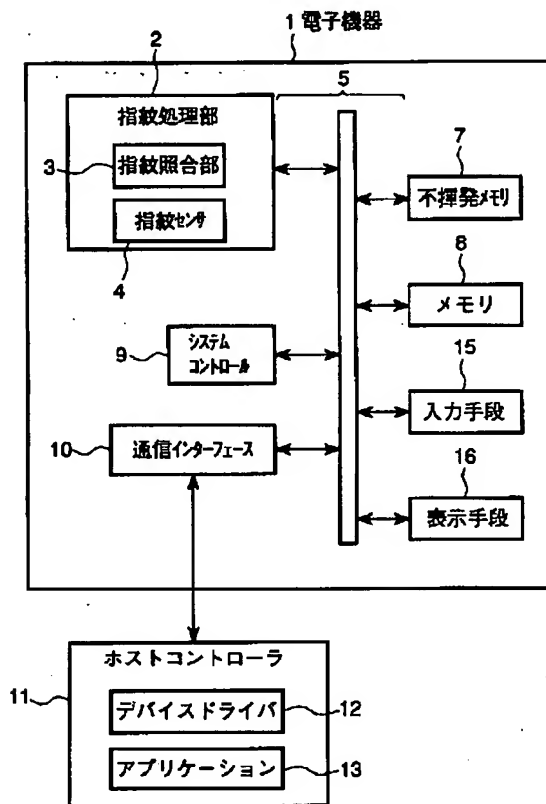
【図1】本発明の第1実施形態としての電子機器及びホストコントローラの構成例を示すブロック図。

【図2】図1の指紋処理部の構成例を示すブロック図。

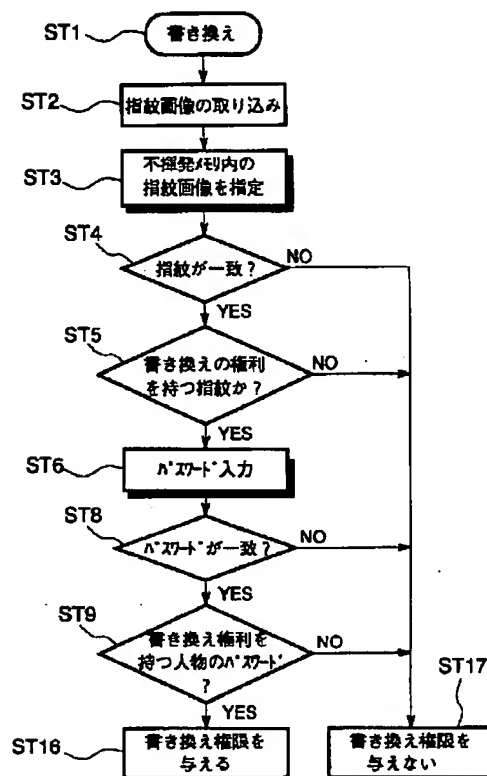
【図3】図1の電子機器のファームウェアの書き換え方法の一例を示すフローチャート。

【図4】図3のフローチャートの変形例を示すフローチャート。

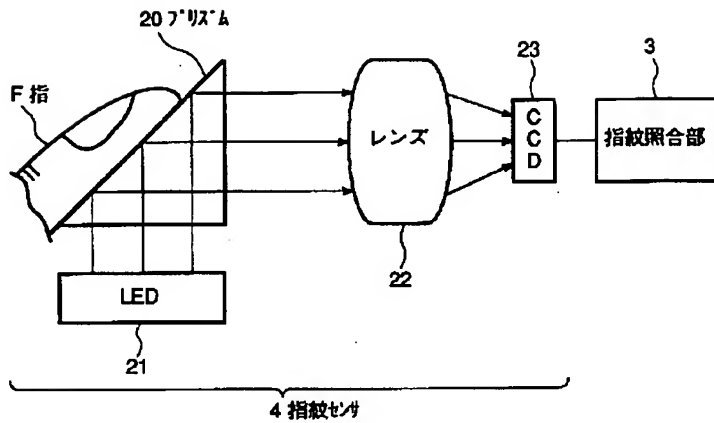
【図1】



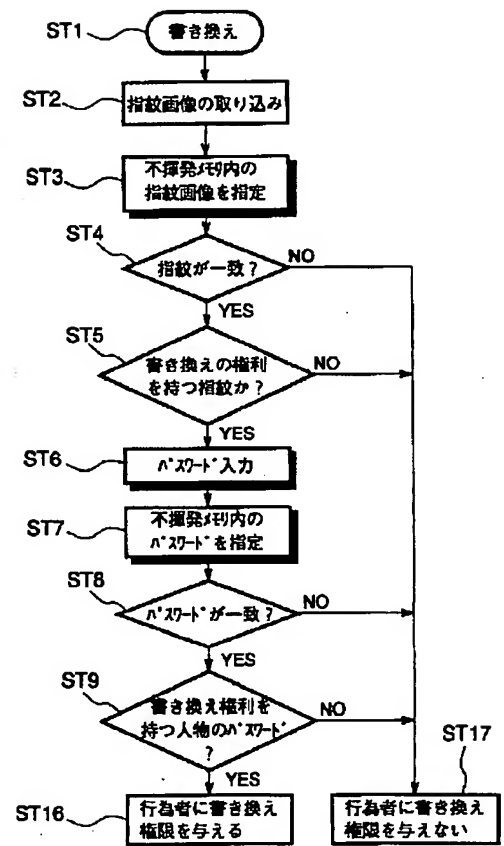
【図3】



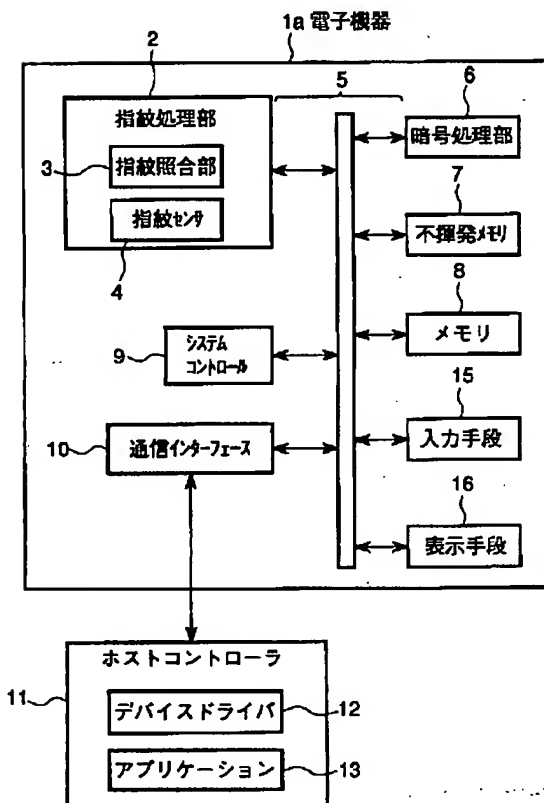
【図2】



【図4】

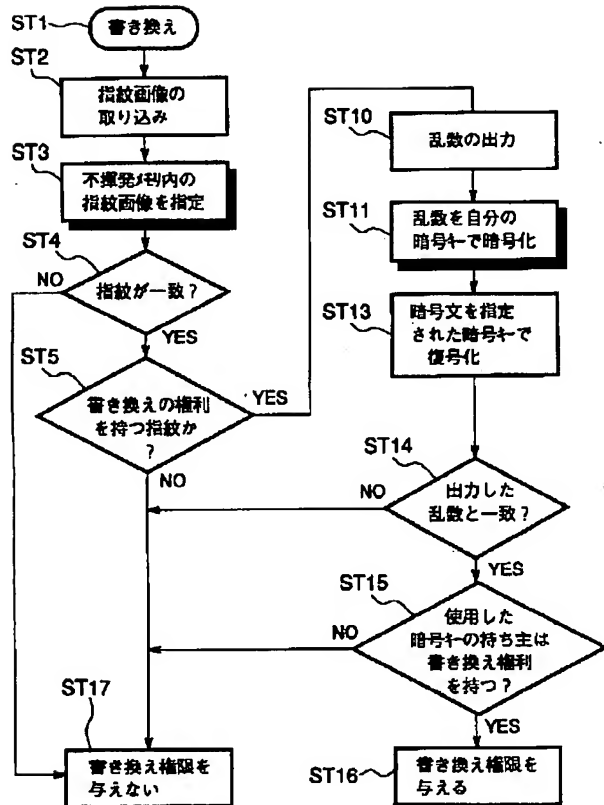


【図5】





【図6】



【図8】

【図7】

